Page 5, line 20, change "input" to --inputted--; and

line 21, change "decrypted" to --broken--.

Page 9, line 24, change "scrambler" to --randomizer--.

Page 10, line 2, change "scrambler" to --randomizer--.

Page 14, line 6, change "decryption" to --cryptanalysis--.

Page 20, line 11, after "this" insert --cryptanalysis--;

line 12, change "decryption" to --cryptanalysis--; and

line 14, change "influence" to --relationship--; and "small" to --weak--.

Page 21, line 14, change "decryption" to --cryptanalysis--; and

line 27, change "decryption" to --cryptanalysis--.

Page 25, line 25, change "decryption" to --cryptanalysis--.

Page 28, line 13, change "decryption" to --cryptanalysis--.

Page 30, line 7, change "decryption" to --cryptanalysis--;

line 14, change "$p^{-1}(a)/p^{-1}(\bar{a})$" to --$P^{-1}(a)/P^{-1}(\bar{a})$--;

A1

line 16, change "$p^{-1}(a)/p^{-1}(\bar{a})$" to --$P^{-1}(a)/P^{-1}(\bar{a})$--;

A2

line 17, change "p-1(a)" to --$P^{-1}(a)$--; and change

A3

"$p^{-1}(\bar{a})$" to --$P^{-1}(\bar{a})$--;

A4

line 24, change "p^{-1}" to --P^{-1}--;

line 25, change "p^{-1}" to --P^{-1}--; and

line 27, change "p^{-1}" to --P^{-1}--; and change

"$p^{-1}(\bar{a})/p^{-1}(\bar{a})$" to --$P^{-1}(a)/P^{-1}(\bar{a})$--.

A5

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D.C. 20005
202-408-4000

Page 31, line 3, change "$p^{-1}(a)/p^{-1}(\bar{a})$" to --$P^{-1}(a)/P^{-1}(\bar{a})$; and

A6

line 10, change "$p^{-1}(\bar{a})/p^{-1}(a)$" to --$P^{-1}(\bar{a})/P^{-1}(a)$;

A7

line 13, change "$p^{1}(b)/p^{-1}(\bar{b})$" to --$P^{-1}(b)/P^{-1}(\bar{b})$--.

A8

Page 32, line 6, change "$\bar{\alpha} = p^{-1}(a)$ and $\bar{\alpha} = p^{-1}(\bar{a})$" to --$\bar{\alpha} = P^{1}(a)$ and $\bar{\alpha} =$

A9

$P^{-1}(\bar{a})$--; and

lines 11 and 12, change "$p^{-1}E^{-1}(\alpha)$ or $p^{-1}E^{-1}(\bar{\alpha})$" to

A10

--$P^{1}E^{-1}(\alpha)$ or $P^{1}E^{-1}(\bar{\alpha})$--.

Page 35, line 22, change "(PC - 1)" to --(PC-1)--;

line 23, change "(PC - 2)" to --(PC-2)--; and

line 25, change "(PC - 1)" to --(PC-1)--.

Page 36, line 2, change "(PC - 2)" to --(PC-2)--; and

line 7, change "PC - 2" to --PC-2--.

IN THE CLAIMS:

Please amend claims 43 and 44 as follows:

Sub B1

43. (Amended) A method according to claim 34, wherein a Hamming weight indicating the number of "1" bits ["1s"] of an n-bit long bit sequence x is defined as H(x), and the Hamming weight H(a) of the mask a satisfies $0 < H(a) < n$.

A11

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D.C. 20005
202-408-4000